UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/901,473 | 07/10/2001 | William Michael Raike | P66409US1 | 5642 |

7590 08/08/2005

JACOBSON HOLMAN
LAW OFFICES
PROFESSIONAL LIMITED LIABILITY COMPANY
400 SEVENTH STREET, N. W.
WASHINGTON, DC 20004

| EXAMINER | |
|---|---|
| UNGAR, DANIEL M | |
| **ART UNIT** | **PAPER NUMBER** |
| 2132 | |

DATE MAILED: 08/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/901,473 | RAIKE ET AL. | |
| | Examiner | Art Unit | |
| | Daniel M. Ungar | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *09 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

*DETAILED OFFICE ACTION*

1. Claims 1-10 have been examined. Appropriate sections of 35 U.S.C. have been quoted in previous Office Actions.

*OBJECTIONS*

2. In light of amendments to the claims, the objections are withdrawn.

*CLAIM REJECTIONS - 35 U.S.C. 112*

3. Claims 1 and 8 recite the limitation, "subsequently." It is not clear subsequent to what the client generates its request.

4. In light of amendments to the claims, the previous rejections under 35 U.S.C. 112, second paragraph are withdrawn.

*RESPONSE TO ARGUMENTS - 35 U.S.C. 103(a)*

5. Regarding the rejections to claims 1, 2, 9, and 10, Applicant argues that there is no motivation to combine the teaching of Lee with the teaching of Peinado. These arguments have been considered fully but are not found persuasive. Although Lee, contrary to Peinado, is concerned with enabling content stored on physical media already in the user's possession, there is still still ample motivation to provide a separate server as the retail conduit ("distribution server") of the media keys, which is the particular teaching of Lee that is relevent to the invention of Peinado. Applicant's argument points out the distinction between Peinado and Lee with regard to the method of delivery of the encrypted **content**, but Examiner's motivation to combine deals with the authorizing the distribution of the **key** (by determining user compliance with conditions, etc.), in which the inventions of Peinado and Lee are similar, so that one of ordinary skill in the art would find motivation to use a particular aspect of Lee in the invention of Peinado. As stated in the prior Office Action, the functionality of the retail server of determining user compliance with conditions, i.e. submitting payment and/or registering personal information (see Lee, column 5, lines 9-13 and 55-63), is distinct from the functionality of the server that handles the media keys, and therefore one would be motivated

to physically separate the servers. For example, system resources of each server may be completely directed to its respective functionality, whereas if one server was performing two distinct applications, neither application would retain full use of the server's resources.

6. With regard to Applicant's argument that the combination of Peinado with Lee does not result in the claimed invention, as amended to include, "subsequently", Examiner respectfully disagrees. Peinado discloses, "the user will attempt to render the digital content" (column 13, line 65), and "the DRM system in fact decrypts the digital content only if the user has a valid license for such digital content" (column 14, lines 53-56). The order in which the content and the key/license are downloaded does not render the invention patentably distinct from the prior art. In both the instant invention and Peinado, the key is what the user must purchase or otherwise comply with certain conditions to obtain, not the encrypted content. In both the instant invention and Peinado, the content can only be played once both the content and key are present, irrespective of how and when each became present.

7. Regarding Applicant's argument to the rejections of claim 3, Examiner respectfully disagrees. Rather than sending the key together with the license acquisition information, as Applicant asserts, Peinado discloses that the information includes **how to obtain the license** from another server, so that the second server may be accessed (see column 18, lines 37-39). Thus the license acquisition information does cause a request to be made of a second server.

8. However, Applicant's argument to the rejection of claim 4 is found to be persuasive. Peinado does not cause the client device to generate a request to the first server to supply the encrypted media work.

9. Regarding the arguments surrounding the rejection to claim 6, Examiner respectfully disagrees. That Blakley relates to encryption for a mass storage device does not disrupt the combination with Peinado. Peinado already suggests storing the key in memory. Peinado only fails to specify volatile memory, and Blakely shows a motivation to use this specific type of

memory. This motivation applies to all applications of encryption, of distributed content as well as mass storage. Thus combination with Peinado is proper.

*CLAIM OBJECTIONS*

10. Claim 4 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

*CLAIM REJECTIONS - 35 U.S.C. 103(a)*

11. Claims 1-5 and 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peinado et al., U.S. Patent Number 6,775,655, filed 11/24/99, in view of Lee et al., U.S. Patent Number 6,636,966, filed 04/03/00.

12. Regarding claims 1, 7, and 8, Peinado et al. disclose a method for the secure distribution of audio-visual media over a network comprising:

encrypting each media work with an encryption key unique to each work (see column 2, lines 48-52);

storing the encrypted media on one or more servers (see column 2, lines 36-52; column 6, line 40; figure 1, item 22);

storing the media keys on a server (see column 2, lines 56-63; column 6, line 41; figure 1, item 20);

a retail server proving consumers the right to media keys in exchange for complying with conditions, the consumer requesting a media key, and the server verifying compliance with conditions, and passing request to the key server (see column 20, line 53 - column 21, line 24; column 19, lines 33-45);

the second server verifying the allowability of fulfilling requests from client and if allowable encrypting the relevant media key and downloading it to the client (see column 21, lines 36-43; column 19, lines 17-45);

encrypting relevant media key and downloading it to the client (see column 3, lines 27-38);

client decrypting the received media key and storing it in memory (see column 21, lines 43-45; figure 4, item 38);

client requesting the desired encrypted media work and downloading it from the server (see column 13, lines 15-33);

client retrieving the media key from memory and using it to decrypt the media work so it can be played (see column 23, lines 45-64);

13. Note that the "black box" detailed by Peinado et al. is client-side. Peinado et al. do not, however, disclose the retail server to be a separate, third server. Rather, the same server that handles the keys handles the retail functions. Nevertheless, Lee et al., in a similar field of endeavor, do disclose a separate server for these functions ("distributor"). This server accepts the client requests, and passes them to a second server, which verifies the requests. Upon verification, the encrypted key is passed to the distribution server, which in turn is downloaded to the client (see embodiment of column 5, lines 9-13 and 16-23). Given the teachings of Lee et al., it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Peinado et al. to provide for a separate retail server to pass the client requests to the server and pass the key to the client in order to further separate differing functions across distinct servers.

14. Regarding claim 2, Peinado et al. disclose storing the media key in memory encrypted, and when the encrypted media work is downloaded, the encrypted media key is retrieved from memory, decrypted, and used to decrypt the media work (see column 23, line 55 - column 24, line 1).

15. Regarding claim 3, Peinado et al. disclose the use of license acquisition information, meeting the claimed limitation of steering files, which correspond to each media work and its corresponding key and contain information identifying the location of the media key (see column 18, line 27-48; column 28, line 41 - column 30, line 29).

16. Regarding claim 5, Peinado et al. disclose encryption using a public key algorithm wherein the client includes the consumer's public key with the request, and the relevant media key is encrypted using the consumer's public key, and the client decrypts it using the consumer's private key (see column 2, lines 48-52; column 3, lines 27-49; column 23, lines 45-64).

17. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peinado et al. in view of Blakley III et al., U.S. Patent Number 5,677,952. Peinado et al. does not disclose storing the key in volatile memory. Blakley III et al., however, do disclose storing an encryption key in volatile memory so that "when the particular computing session is ended or interrupted, the secret key is erased from the computer's volatile memory to prevent unauthorized access to and disclosure of the information in the sector". It would have been an obvious modification to the method of Peinado et al. to store the key in volatile memory to prevent unauthorized access after the computing session is ended.

18. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peinado et al. in view of Lee et al. Peinado et al. disclose a method for the secure distribution of digitized audio-visual media to consumers over a data network comprising:

encrypting each media work with a unique encryption key (see column 2, lines 48-52);

storing the encrypted media on a first server (see column 2, lines 36-52; column 6, line 40; figure 1, item 22);

storing the media keys on a second server (see column 2, lines 56-63; column 6, line 41; figure 1, item 20);

creating steering files (license acquisition information) corresponding to each work and its corresponding key, identifying the media work and the location of the media key, the steering files when executed on a network-connected client causing a request to be made to the second server for the key (see column 18, line 27-59; column 28, line 41 - column 30, line 29);

the key server verifying allowability of fulfilling client's request and if allowable encrypting the media key with a key unique to the consumer and downloading it to the client (see column 21, lines 36-43; column 19, lines 17-45);

decrypting the product key at the client device and storing it in memory (see column 21, lines 43-45; figure 4, item 38);

generating a request to the first server from the client to deliver the product identified in the steering file, and downloading the encrypted product from the server to the client (see column 13, lines 15-33);

retrieving the product key from memory and using it to decrypt the product to a condition where it is ready for use (see column 23, lines 45-64).

19. Peinado et al. do not, however, disclose the steering files to be on a separate, third, server. Nevertheless, Lee et al., in a similar field of endeavor, do disclose a separate server (see embodiment of column 5, lines 9-13 and 16-23). Given the teachings of Lee et al., it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Peinado et al. to provide for a separate server to make available steering files to the client in order to further separate differing functions across distinct servers.

20. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peinado et al. in view of Lee et al. Peinado et al. disclose a method for the secure distribution of digitized products to consumers over a data network comprising:

encrypting each product with a unique encryption key (see column 2, lines 48-52);

storing the encrypted product on a first server (see column 2, lines 36-52; column 6, line 40; figure 1, item 22);

storing the product keys on a second server (see column 2, lines 56-63; column 6, line 41; figure 1, item 20);

creating steering files (license acquisition information) corresponding to each product and its corresponding key, identifying the product and the location of the

product key, the steering files when executed on a network-connected client causing a request to be made to the second server for the key (see column 18, line 27-59; column 28, line 41 - column 30, line 29);

the key server encrypting the product key with a key unique to the consumer and downloading it to the client (see column 18, line 27-48);

decrypting the product key at the client device and storing it in memory (see column 21, lines 43-45; figure 4, item 38);

generating a request to the first server from the client to deliver the product identified in the steering file, and downloading the encrypted product from the server to the client (see column 13, lines 15-33);

retrieving the product key from memory and using it to decrypt the product to a condition where it is ready for use (see column 23, lines 45-64).

21. Peinado et al. do not, however, disclose the steering files to be on a separate, third, server. Nevertheless, Lee et al., in a similar field of endeavor, do disclose a separate server (see embodiment of column 5, lines 9-13 and 16-23). Given the teachings of Lee et al., it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Peinado et al. to provide for a separate server to make available steering files to the client in order to further separate differing functions across distinct servers.

*CONCLUSION*

22. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel M. Ungar whose telephone number is 571.272.7960. The examiner can normally be reached on 8:30 - 6:00 Monday - Thursday, Alt. Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571.272.3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Art Unit 2132

DMU

Daniel M. Ungar

Gilberto Barron

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100